UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,437	01/14/2002	David Carroll Challener	RPS9 2001 0142	2954

47052 7590 01/13/2006

SAWYER LAW GROUP LLP
PO BOX 51418
PALO ALTO, CA 94303

EXAMINER	
GURSHMAN, GRIGORY	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/046,437	CHALLENER, DAVID CARROLL	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/28/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's amendment has overcome the rejection of claims 1, 7, 16 and 22 under 35 USC § 112. Accordingly the rejection of the instant claims is withdrawn.

2. With regard to the rejection of claims 3, 7, 18, 22 and 24 under 35 USC § 112 second paragraph, Applicant argues that generating a random number by hashing the pass phrase is possible if there is enough entropy. Examiner respectfully disagrees and points out that the number produced will be a pseudo-random number and should be recited as such in the instant claims.

3. With respect to claims 1-30, and the independent claims 1, 7, 16 and 22 in particular, Applicant argues that the claimed invention is different form the one of Oorschot, because Oorschot does not teach the double encryption of the keys. Examiner respectfully disagrees with this assessment of teachings of Oorschot. Oorschot in fact does teach the limitations "creating a migratabale keyblob... wherein the migratable keyblob contains a key" is met by encrypted block of data having A and B headers (see Fig. 1); and the limitation "wrapping the migratable keyblob with a public key of the key's parent key" is met by Fig. 1, depicting encryption of the symmetric key K by A and B public encryption keys.

4. Applicant's arguments with respect to the independent claims 1, 7, 16 and 22 have not been found persuasive in view of the fact that the limitations of the instant claims are met by Oorschot. The combination of Oorschot and Eldridge renders the claims 1-30 obvious. Accordingly the rejections of claims 1-30 are maintained

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

6. Claims 3, 7, 18, 22, 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim. The limitation "generating a ... random number by hashing the pass phrase" renders the instant claims indefinite, because hashing the pass phrase will not produce a random number. Based on the pass phrase and the hash function used the number produced will be definite or pseudo-random, but not *random*.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1- 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oorschot (U.S. Patent No. 5.850.443) in view of Eldridge (U.S. Patent No. 6.061.799).

9. Referring to the instant claims, Oorschot discloses a key management system for mixed-trust environments (see abstract). Oorschot teaches that symmetric key is encrypted using asymmetric technique, and along with this transporting ciphertext derived from plaintext encrypted under this symmetric key (see abstract and Fig. 1).

10. Referring to the independent claims 1, 7, 16 and 22, the limitation "creating a migratabale keyblob... wherein the migratable keyblob contains a key" is met by encrypted block of data having A and B headers (see Fig. 1). The limitation "wrapping the migratable keyblob with a public key of the key's parent key" is met by Fig. 1, depicting encryption of the symmetric key K by A and B public encryption keys. The limitation "migrating the migratable keyblob" is met by sending the encrypted message with the headers from entity A (Fig. 3) to entity B (Fig. 4). Oorschot, however, does not explicitly teach encrypting the random number with a pass phrase for a user.

11. Referring to the instant claims, Eldridge discloses a removable media for password based authentication (see abstract). Eldridge teaches that the medium contains keys at least partially derived from the passwords. The computer system with which the portable medium interfaces determines whether any of the data associated with the passwords matches authentication data previously stored in the computer system and associated with the client process (see abstract). According to Eldridge, key 308 is generated by a process illustrated conceptually in FIGS. 3B and 4. Referring to FIG. 3B, secret parameter 302 and one of the passwords, illustrated here as current password 304, are combined, e.g., concatenated, together and supplied to a pseudo-random number generator 320. The data output generated by pseudo-random number

generator 320 serves as a key 308. A pseudo-random number generator will produce the same output data for the same given input data each time. Conversely, a completely random number generator will produce, theoretically, a different data output for the same input data every time.

12. Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the key management system of Oorschot, using the encryption (i.e. wrapping) of the key with the public key, by having the key generated by combing the password with the random number as taught in Eldridge. One of ordinary skill in the art would have been motivated to modify the key management system of Oorschot, using the encryption (i.e. wrapping) of the key with the public key, by having the key generated by combing the password with the random number as taught in Eldridge for determining whether any of the data associated with the passwords matches authentication data previously stored in the computer system and associated with the client process (see Eldridge, abstract).

13. Referring to claims 3, 4, 5, 7, 18, 20, and 22, Eldridge teaches that random number generator will produce different random numbers each time, which meets the limitations of the instant claims reciting second, third and etc. random numbers.

14. Referring to claims 4, 12, 20, the limitation "unwrapping the migratable keyblob by the secure chip using the secure chip private key" is met by private key decryption (see Figs. 2 and 4).

15. Referring to claims 2, 8, 11, 17, 23, 29 Oorschot teaches using XOR operation applied to different keys (see column 7, lines 1-13). Eldridge teaches combining the

random number with the key. One of ordinary skill in the art would have been motivated to use XOR operation for combing the random number with the key for creating the higher security level of the encrypted information.

16. Referring to claims 3, 10, 13, 18, 20, 25, it is well known in the art to use mask generation function MGF – see Applicant's disclosure lines 0020. One of ordinary skill in the art would have been motivated to use MGF for generation of the random number based on the given number since it is quick and efficient way to generate a random number.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

G.G.

GG

Grigory Gurshman
Examiner
Art Unit 2132

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100